

PATENT ABSTRACTS OF JAPAN

W 926

(11)Publication number : 2001-256004

(43)Date of publication of application : 21.09.2001

(51)Int.Cl.

G06F 3/06
G06F 1/00
G06F 12/14
G11B 20/10

(21)Application number : 2000-069822

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 14.03.2000

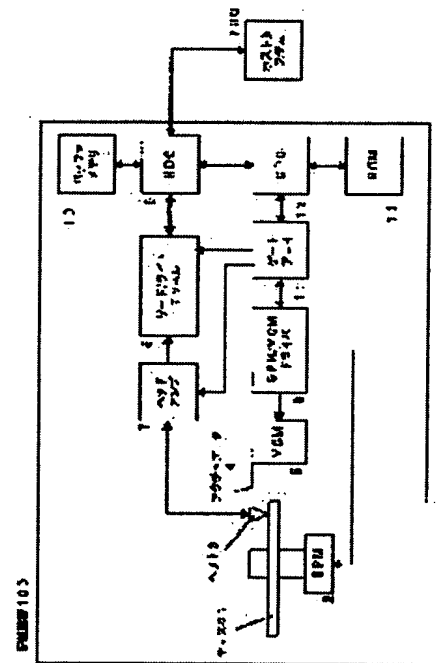
(72)Inventor : IGARI CHIKASHI

(54) INFORMATION STORAGE AND REPRODUCTION SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To enable restriction of access of a host system to user data in a storage device with respect to the storage device to be attachably/detachably connected with the host system.

SOLUTION: Authentication data for access control to be used in judgment of propriety of the access of the host system to the user data in the storage device are created in cooperation with the storage system and the host system and stored in both. And the storage device controls the access of the host system to the user data in the storage device based on the authentication data for access control stored in the host system and the authentication data for access control stored in the storage device in the case of judgment of the propriety of the access.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(43)公開日 平成13年9月21日(2001.9.21)

(51)Int.Cl. ⁷		識別記号	F I	データベース*(参考)	
G 0 6 F	3/06	3 0 4	G 0 6 F	3/06	3 0 4 H 5 B 0 1 7
	1/00	3 7 0		1/00	3 7 0 E 5 B 0 6 5
	12/14	3 2 0		12/14	3 2 0 A 5 D 0 4 4
G 1 1 B	20/10		G 1 1 B	20/10	H

審査請求 未請求 請求項の数9 O.L (全 15 頁)

(21)出願番号 特願2000-69822(P2000-69822)

(22)出題日 平成12年3月14日(2000.3.14)

(71)出題人 000003078

株式会社東芝

東京都港区芝浦一丁目1番1号

(72) 発明者 猪狩 史

東京都青梅市末広町2丁目9番地 株式会社東芝青梅工場内

(74) 代理人 100083161

弁理士 外川 英明

Fターム(参考) 5B017 AA03 BA05 BA09 CA06 CA14

5B065 BA01 PA06 PA14 ZA03

5D044 AB01 CC04 DE48 EF05 FG18

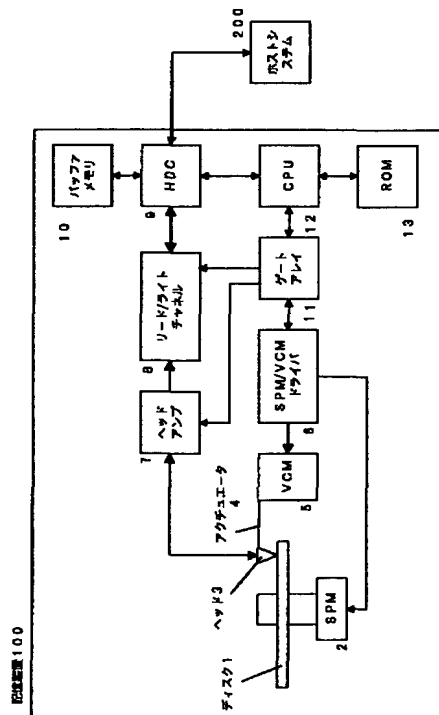
GK12 HL01

(54) 【発明の名称】 情報記憶再生システム

(57) 【要約】

【課題】 ホストシステムに着脱可能に接続される記憶装置において、記憶装置のユーザデータに対するホストシステムのアクセスを制限することを可能とする。

【解決手段】 記憶装置のユーザデータへのホストシステムのアクセス可否の判断において使用されるアクセス制御用認証データを、記憶装置とホストシステムとで共同して作成し、双方で記憶する。そして、アクセス可否の判断に際しては、記憶装置が、ホストシステムに記憶されているアクセス制御用認証データと記憶装置に記憶されているアクセス制御用認証データとに基づいて、記憶装置のユーザデータへのホストシステムのアクセス制御を行なう。



【特許請求の範囲】

【請求項 1】 ユーザデータを記憶する記憶装置と、前記記憶装置を着脱可能に接続し前記記憶装置の前記ユーザデータへのアクセスを行なうホストシステムとを有する情報記憶再生システムにおいて、

前記ホストシステム及び前記記憶装置は、前記ホストシステムが作成した認証データに基づいて前記記憶装置が作成した前記ホストシステムの前記ユーザデータへのアクセスを制御するためのアクセス制御用認証データ、又は、前記記憶装置が作成した認証データに基づいて前記ホストシステムが作成した前記アクセス制御用認証データを記憶する認証データ記憶手段をそれぞれ具備し、前記記憶装置は、前記ホストシステムの前記認証データ記憶手段に記憶されたアクセス制御用認証データと、前記記憶装置の前記認証データ記憶手段に記憶されたアクセス制御用認証データとに基づいて、前記ホストシステムからの前記ユーザデータへのアクセスを制御する制御手段を具備することを特徴とする情報記憶再生システム。

【請求項 2】 前記ホストシステムは、当該ホストシステムの固有情報に基づき前記認証データ又は前記アクセス制御用認証データを作成することを特徴とする請求項 1 記載の情報記憶再生システム。

【請求項 3】 前記記憶装置は、当該記憶装置の固有情報に基づき前記認証データ又は前記アクセス制御用認証データを作成することを特徴とする請求項 1 記載の情報記憶再生システム。

【請求項 4】 ユーザデータを記憶する記憶装置と、前記記憶装置を着脱可能に接続し前記記憶装置の前記ユーザデータへのアクセスを行なうホストシステムとを有する情報記憶再生システムにおいて、

前記ホストシステムは、前記ホストシステム側の認証データであるホスト認証データを作成するホスト認証データ作成手段と、

前記ホストシステムの前記ユーザデータへのアクセスを制御するためのアクセス制御用認証データを記憶する第 1 の認証データ記憶手段とを具備し、

前記記憶装置は、

前記ホストシステムの前記ホスト認証データ作成手段により作成された前記ホスト認証データに基づいて前記アクセス制御用認証データを作成するアクセス制御用認証データ作成手段と、

前記アクセス制御用認証データ作成手段により作成された前記アクセス制御用認証データを記憶する第 2 の認証データ記憶手段と、

前記ホストシステムの前記第 1 の認証データ記憶手段に記憶されたアクセス制御用認証データと、前記第 2 の認証データ記憶手段に記憶されたアクセス制御用認証データとに基づいて、前記ホストシステムからの前記ユーザデータへのアクセスを制御する制御手段とを具備するこ

とを特徴とする情報記憶再生システム。

【請求項 5】 前記ホスト認証データ作成手段は、前記ホストシステムの固有情報に基づいて前記ホスト認証データを作成することを特徴とする請求項 4 記載の情報記憶再生システム。

【請求項 6】 前記アクセス制御用認証データ作成手段は、前記ホストシステムの前記ホスト認証データ作成手段により作成された前記ホスト認証データと前記記憶装置の固有情報に基づいて前記アクセス制御用認証データを作成することを特徴とする請求項 4 記載の情報記憶再生システム。

【請求項 7】 ユーザデータを記憶する記憶装置と、前記記憶装置を着脱可能に接続し前記記憶装置の前記ユーザデータへのアクセスを行なうホストシステムとを有する情報記憶再生システムにおいて、

前記ホストシステムは、前記記憶装置で作成される記憶装置認証データに基づいて前記ホストシステムの前記ユーザデータへのアクセスを制御するためのアクセス制御用認証データを作成するアクセス制御用認証データ作成手段と、

前記アクセス制御用認証データ作成手段により作成された前記アクセス制御用認証データを記憶する第 1 の認証データ記憶手段とを具備し、

前記記憶装置は、

前記記憶装置側の認証データである前記記憶装置認証データを作成する記憶装置認証データ作成手段と、

前記ホストシステムで作成された前記アクセス制御用認証データを記憶する第 2 の認証データ記憶手段と、

前記ホストシステムの前記第 1 の認証データ記憶手段に記憶されたアクセス制御用認証データと、前記第 2 の認証データ記憶手段に記憶されたアクセス制御用認証データとに基づいて、前記ホストシステムからの前記ユーザデータへのアクセスを制御する制御手段とを具備することを特徴とする情報記憶再生システム。

【請求項 8】 前記アクセス制御用認証データ作成手段は、前記記憶装置で作成される前記記憶装置認証データと前記ホストシステムの固有情報に基づいて前記アクセス制御用認証データを作成することを特徴とする請求項 7 記載の情報記憶再生システム。

【請求項 9】 前記記憶装置認証データ作成手段は、前記記憶装置の固有情報に基づいて前記記憶装置認証データを作成することを特徴とする請求項 7 記載の情報記憶再生システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、ユーザデータを記憶する記憶装置とこの記憶装置を着脱可能に接続してアクセスを行なうホストシステムとを有する情報記憶再生システムに関し、記憶装置側において、記憶装置にアクセスするホストシステムを特定のものに限定可能とする

情報記憶再生システムに関する。

【0002】

【従来の技術】近年のハードディスクドライブ（HDD）やCD-ROM等の記憶装置は、パーソナルコンピュータ等のホストシステムに、着脱可能な形態で使用できるようになっており、例えば、現在接続しているホストシステムから記憶装置を取り外して別のホストシステムに接続して使用することも可能である。

【0003】このため、他のホストシステムが記憶装置をアクセスすることが可能であり、セキュリティ上の問題点があった。

【0004】この問題点を解決するために、従来では、記憶装置に対するホストシステムからのアクセスを制限するためのセキュリティ方式が実現されている。この従来のセキュリティ方式は、ホストシステムが作成したパスワード（ホストシステムにおいてユーザが入力する）を予め記憶装置に記憶しておく。そして、ホストシステムから記憶装置へのアクセスが行なわれる際に、記憶装置において、ホストシステムから送信されるパスワード（ホストシステムにおいてユーザが入力する）が記憶装置に予め記憶されているものと一致するか否かを判断し、一致する場合にホストシステムに対してアクセスを許可するという方式をとっている。

【0005】しかしこのセキュリティ方式では、ホストシステムが違っていてもホストシステムから記憶装置に送信されるパスワードが合っていれば、ホストシステムの違いに関係なく記憶装置はアクセスを許可することとなる。従って、記憶装置に予め記憶されているパスワードが他人に知られてしまうと、他人により別のホストシステムから不正にアクセスできてしまうといった課題がある。

【0006】また、記録媒体に記録されたユーザデータへのアクセスを制御する技術としては、特開平11-224456号に、光ディスクに対する情報処理装置のアクセスを制御する方法が記載されている。この従来技術では、情報処理装置に、光ディスクのIDとこの光ディスクにアクセスした際に発生する乱数を記憶し、一方、光ディスクに、上記したものと同様の乱数と情報処理装置のIDを記憶しておく。そして、情報処理装置が光ディスクに再度アクセスする時に、情報処理装置が、双方に記憶された3つの情報（光ディスクのID、乱数、情報処理装置のID）が全て一致するか否かを判断し、一致しない場合には光ディスクのアクセスを拒絶するようにしている。

【0007】しかしこの方式は、アクセスの行なわれる側である光ディスクでは情報処理装置からのアクセスを制御できない。従って、例えば、上述した制御を無視して光ディスクにアクセスするよう不正に構成された情報処理装置が用いられ、光ディスクに不正にアクセスが行なわれた場合、光ディスク側ではその情報処理装置から

の不正アクセスを抑制することができない。

【0008】

【発明が解決しようとする課題】このように、従来のセキュリティ方式は、アクセスしようとするホストシステムの違いに関係なくパスワードが合っていれば記憶装置へのアクセスを許可していたため、他人が不正にパスワードを知り、そのパスワードを用いて他人の所有するホストシステムから不正にアクセスされる可能性があるが、その他人の所有するホストシステムからの不正アクセスを抑制することができないという課題があった。また、特開平11-224456号に記載された方式では、アクセスする側の情報処理装置により不正アクセスが行なわれると、アクセスされる側の光ディスクではその不正アクセスを抑制できないという課題があった。

【0009】本発明は上記の事情を考慮してなされたもので、記憶装置側において、当該記憶装置へのアクセスを特定のホストシステムにのみに制限することが可能な記憶装置及びホストシステムを有する情報記憶再生システムを提供することを目的とする。

【0010】

【課題を解決するための手段】本発明の情報記憶再生システムは、ホストシステム及び記憶装置の各々の認証データ記憶手段に、ホストシステムが作成した認証データに基づいて前記憶装置が作成した前記アクセス制御用認証データ、又は、記憶装置が作成した認証データに基づいてホストシステムが作成したアクセス制御用認証データを記憶する。そして、記憶装置の制御手段において、ホストシステムに記憶されたアクセス制御用認証データと、記憶手段に記憶されたアクセス制御用認証データとに基づいて、ホストシステムからのユーザデータへのアクセスを制御する。

【0011】このように、ホストシステムと記憶装置との両方により作成したアクセス制御用認証データを用いることにより、記憶装置のユーザデータへのアクセスを特定のホストシステムにのみに制限することが可能となる。

【0012】

【発明の実施の形態】（記憶装置の構成）先ず、本実施形態の記憶装置の構成を説明する。ここで、記憶装置は、例えば、HDD、FDD等の磁気ディスク装置や、DVD、MO、CD-ROM、MD等の光磁気ディスク装置、磁気テープ記憶装置、半導体メモリを用いた記憶装置等、ホストシステムに着脱可能に接続され使用されるものである。

【0013】本実施形態では、記憶装置として、図1に示すように、HDDを想定している。HDDは、大別してユーザデータを記憶する記憶媒体としてのディスク1と、データのリード／ライト動作を実行するためのヘッド3と、リード／ライトデータの信号処理系と、制御系とから構成されている。ディスク1は、スピンドルモータ

タ (SPM) 2 により回転される。ヘッド 3 は、通常ではリードヘッドとライトヘッドとが同一スライダ上に実装されている。ヘッド 3 は、アクチュエータ 4 に搭載されて、ディスク 1 の半径方向に移動される。アクチュエータ 4 は、ボイスコイルモータ (VCM) 5 を駆動源として、回転駆動するように構成されている。SPM 2 及び VCM 5 は、後述する CPU 12 の制御により、SPM/VCM ドライバ 6 から駆動電流を供給されて駆動する。SPM/VCM ドライバ 6 は、通常では CPU 12 からゲートアレイ 11 を介してデジタルの制御値を入力し、当該制御値に応じて駆動電流を出力する。

【0014】信号処理系は、ヘッドアンプ 7 及びリード/ライトチャネル 8 を有する。ヘッドアンプ 7 は、ヘッド 3 から読み出されたリード信号を増幅してリード/ライトチャネル 8 に送出する。また、ヘッドアンプ 7 は、リード/ライトチャネル 8 で処理されたライト信号 (符号化された記録データ) を電流に変換してヘッド 3 に供給する。リード/ライトチャネル 8 は、エンコーダ及びデコーダを有し、ホストシステム 200 からの書き込みデータをライト信号に変換し、且つ、ディスク 1 から読み出されたリード信号を元の書き込みデータに復号化するための各種信号処理を実行する。

【0015】制御系は、ハードディスクコントローラ (HDC) 9 と、CPU 12 と、ゲートアレイ 11 とを有する。HDC 9 は、ホストシステム 200 との間でのデータ転送を制御するものであり、ホストシステム 200 から入力されるデータを一次的にバッファメモリ 10 に記憶させる等といった制御を行う。また、HDC 9 は、図 2 に示すように、ATA コマンドの実行に必要な各種のレジスタを有する。CPU 12 は、ROM 13 に格納された制御プログラムに従って、後述する本実施形態の認証処理を実行する。ゲートアレイ 11 は、主として CPU 12 の制御信号、及びリード/ライトチャネル 8 からのサーボデータの入出力を制御するインターフェース制御回路に相当する。

(記憶装置側の認証処理) 以下、記憶装置側の認証処理について説明する。

【0016】図 2 に示すように、ATA インターフェース仕様の HDC 9 は、コマンドの実行処理に必要な各種のレジスタを有しているが、これら各種のレジスタの内、本実施形態の認証処理で使用されるレジスタは、コマンドレジスタ、セクタカウントレジスタ、エラーレジスタである。コマンドレジスタは、ホストシステム 200 から送信される各種のコマンドを記憶する。セクタカウントレジスタは、ホストシステム 200 から送信されるデータサイズ、及び、記憶装置 100 から送信するデータサイズを示す情報を記憶する。エラーレジスタは、ホストシステム 200 から送信されたコマンドに対する記憶装置 100 の応答を示す情報を記憶する。

【0017】以下、記憶装置側の認証処理を説明する。

ここで、記憶装置 100 における認証処理は、記憶装置 100 に対して、ホストシステム 200 側から電源投入が行なわれた後に実行されるものであり、ホストシステム 200 から送信される各種のコマンドに応答する形態で実行される。

(記憶装置の第 2 次認証データの記憶有無の確認動作)

図 3 は、ホストシステム 200 に対して第 2 次認証データの記憶有無の応答を行なう記憶装置における処理を示すフローチャートである。

【0018】第 2 次認証データは、記憶装置 100 とホストシステム 200 とが双方の固有情報を用いて共同で作成した認証データであり、記憶装置 100 では、双方に記憶されている第 2 次認証データの比較を行うことで、ホストシステム 200 に対してアクセス許可を行うか否かを判断する。また、ここでは、記憶装置 100 とホストシステム 200 のいずれも第 2 次認証データを記憶していない場合を想定して、以下に説明する。

【0019】先ず、記憶装置 100 に対して、ホストシステム 200 から、記憶装置 100 側に第 2 次認証データが記憶されているか否かを確認するため、認証データ確認コマンド (8Dh) が送信されると、記憶装置 100 の HDC 9 では、そのコマンドレジスタに認証データ確認コマンド (8Dh) が書き込まれた状態となる。

【0020】なお、ここでは認証コマンドを、(8Dh) という 3 文字の文字コードの組合わせを例として説明しているが、現在 ATA コマンドに採用されている 3 文字の文字コードの組合わせ以外の組合わせであれば何でもよい。また、以降の説明で、ホストシステム 200 が送信する様々なコマンドを、所定の 3 文字の文字コードの組合わせで例示しているが、これは現在 ATA コマンドで採用されている 3 文字の文字コードの組合わせ以外から例として示したものであり、これ以外でも現在 ATA コマンドで採用されていないものであれば、どのような組合わせでも良い。

【0021】HDC 9 のコマンドレジスタに認証データ確認コマンド (8Dh) が書き込まれた状態となると、記憶装置 100 の CPU 12 は、HDC 9 のコマンドレジスタから認証データ確認コマンド (8Dh) を読出し (ステップ S1)、コマンド内容を確認する (ステップ S2)。コマンドが認証データ確認コマンド (8Dh) でない場合は、読み出された別のコマンドに対応した処理を行なうが (ステップ S2 の No)、この場合は認証データ確認コマンド (8Dh) であると確認されるため (ステップ S2 の Yes)、次いで、CPU 12 は、第 2 次認証データが記憶されているか否かを確認し、その確認結果を HDC 9 のエラーレジスタに書き込む (ステップ S3)。ここで、第 2 次認証データは、ディスク 1、ROM 13 (フラッシュ ROM 等の書き込みの行える ROM)、CPU 12 内の図示しない RAM のいずれに記憶しても構わないが、本実施形態では、例と

して、ROM13に記憶することとする。この場合、CPU12は、ステップS3において、ROM13に第2次認証データが記憶されているか否かを確認し、その確認結果をHDC9のエラーレジスタに書き込む。このHDC9のエラーレジスタには認識結果を示す情報として、第2次認証データが記憶されている場合は、(00h)がセットされ、一方、記憶されていない場合は(04h)がセットされる。ここでは、記憶装置100とホストシステム200のいずれも第2次認証データを記憶していない場合を想定しているため、記憶装置100のROM13には第2次認証データが記憶されておらず、CPU12は、第2次認証データが記憶されていないことを示す情報(04h)をエラーレジスタに書き込む。この時のHDC9の各レジスタの記憶内容を、図2に示している。CPU12は、確認結果をエラーレジスタに書き込むと、ホストシステム200から送信された認証データ確認コマンド(8Dh)に対する処理を終了する。

【0022】この結果、ホストシステム200側では、HDC9のエラーレジスタの記憶内容(04h)を読み出すことで、記憶装置100に第2次認証データが記憶されていないことが認識されることとなる。その後、ホストシステム200側では、ホストシステム200自身に第2次認証データが記憶されているか否かを確認する処理が行われ、ホストシステム200側に第2次認証データが記憶されていないと判断された場合は、ホストシステム200側は、記憶装置100との間に新たな接続関係を成立させることで記憶装置100にアクセス可能にすべく、第2次認証データの作成を行なう処理が行われる。

【0023】一方、ホストシステム200側に第2次認証データが記憶されていると判断された場合には、ホストシステム200側で、記憶装置100へのアクセスを実行しない処理が行われることとなる。即ち、この場合、ホストシステム200は、他の記憶装置に対してアクセスが許可された状態にある。本発明では、特定のホストシステムのアクセスを、特定の記憶装置にのみに限定するよう制御を行なうようにしている。このため、ホストシステム200は、アクセスが許可されている他の記憶装置以外とはアクセスしないようにするため、今回アクセスしようとしている記憶装置100へのアクセスを不許可とする。なお、ここで説明したホストシステム200側の処理については、後に詳述する。

【0024】ここでは、ホストシステム200側も第2次認証データが記憶されていないので、ホストシステム200側において、記憶装置100との間に新たな接続関係を成立させ記憶装置100にアクセスできるようにするため、第2次認証データを作成する処理がとられることとなる。このホストシステム200側の第2次認証データ作成処理に対応して、記憶装置100側では次に

説明する第2次認証データ作成動作を行なう。

【0025】(記憶装置側の第2次認証データの作成動作) 記憶装置100側の第2次認証データの作成動作について、図4に示すフローチャートを参照して説明する。

【0026】ホストシステム200が第2次認証データを作成する処理に移った場合、まず、ホストシステム200から記憶装置100に対して、送信すべき第1次認証データのデータサイズを示す情報(01h)が送信され、続いて、第1次認証データ送信コマンド(8Fh)が送信される。ホストシステム200から、第1次認証データのデータサイズを示す情報(01h)、及び、第1次認証データ送信コマンド(8Fh)が送信されると、図5のように、HDC9のセクタカウントレジスタに(01h)、コマンドレジスタに(8Fh)がそれぞれ書き込まれる。ここでは、第1次認証データのデータサイズが512バイトであるため、その旨を示す情報として(01h)が送信される。

【0027】CPU12では、HDC9のコマンドレジスタから第1次認証データ送信コマンド(8Fh)を読み出し(ステップS11)、コマンド内容を確認する(ステップS12)。コマンドが第1次認証データ送信コマンド(8Fh)でない場合は、読み出された別のコマンドに対応する処理を行なうが(ステップS12のNo)、この場合は第1次認証データ送信コマンド(8Fh)であると確認されるため(ステップS12のYes)、ホストシステム100から送信される第1次認証データを受信してバッファメモリ10に記憶する。CPU12は、受信した第1次認証データにエラーがないことを確認すると、HDC9のエラーレジスタの内容を(00h)とし、エラーがない旨をホストシステム200に知らせる(ステップS13)。

【0028】第1次認証データは、例えば、図6に示すように、ホストシステム200において、当該ホストシステム200の固有情報と、第1次認証データを作成する時の日時情報とに基づいて作成されたものである。この例では、ホストシステム200の固有情報として、メーカー名(TOSHIBA)、機種名(Satellite2550X)、シリアル番号(99017796)を使用している。また、日時情報(1999-09-13, 19:40:00)を使用している。第1次認証データは、512バイト(0000h~01FFh)で構成されるが、図6では、その中の0000h~0020hに上記した固有情報を示すデータが記述され、その後の0030h~01FFhにはデータの記述がなく全て「00h」となっている。勿論、この0030h~01FFhにもデータが記述されるような更に長い第1次認証データを作成することも可能である。

【0029】続いて、CPU12は、ホストシステム200から送信された第1次認証データと記憶装置100の固有情報から、第2次認証データを作成する(ステッ

プS14)。ここで、記憶装置100の固有情報は、ディスク1、ROM13、CPU12内の図示しないRAMのいずれに記憶しても構わないが、本実施形態では、ROM13に記憶することとする。CPU12において作成される第2次認証データを、図7に示している。第2次認証データのデータサイズは512バイトであり、その前半の256バイト(0000h~00FFh)がホストシステム200側で作成された第1次認証データであり、後半の256バイト(0100h~01FFh)に記憶装置200の固有情報を付加した形式としている。記憶装置100の固有情報は、メーカー名(TOSHIBA)、機種名(MK6411MAT)、シリアル番号(Z8G50891G)である。作成した第2次認証データは、一次的にCPU12内の図示しないRAMに記憶する。

【0030】CPU12は、第2次認証データを作成すると、ホストシステム200にエラー無く第2次認証データを作成したことを報知すべくHDC9のエラーレジスタに(04h)をセットし、ホストシステム200から送信された第1次認証データ送信コマンド(8Fh)に対する処理を終了する。

(第2次認証データの送信) 図8に示すフローチャートを参照して、記憶装置側の第2次認証データの送信動作を説明する。

【0031】ホストシステム200から第2次認証データの送信を要求すべく、記憶装置100に対して、送信すべき第2次認証データのデータサイズ(512バイト)を示す情報(01h)が送信され、続いて、第2次認証データ受信コマンド(81h)が送信される。この時、図9のように、HDC9のセクタカウトレジスタには(01h)、コマンドレジスタに第2次認証データ受信コマンド(81h)が書き込まれる。

【0032】CPU12は、HDC9のコマンドレジスタから第2次認証データ受信コマンド(81h)を読み出し(ステップS21)、コマンド内容を確認する(ステップS22)。コマンドが第2次認証データ受信コマンド(81h)でない場合は、読み出された別のコマンドに対する処理を行なうが(ステップS22のNo)、この場合は第2次認証データ受信コマンド(81h)であると確認されるため(ステップS22のYes)、CPU12は、ホストシステム200へ第2次認証データを送信することを報知するためにHDC9のエラーレジスタに(00h)をセットした後、CPU12内の図示しないRAMに記憶している第2次認証データをホストシステム200へ送信し、また、ホストシステム200への第2次認証データの送信を終了した後、当該第2次認証データをROM13に記憶する(ステップS23)。ステップS23の処理を行うとCPU12は、ホストシステム200から送信された第2次認証データ受信コマンド(81h)に対する処理を終了する。

【0033】この後、ホストシステム200側では、記

憶装置100が送信した第2次認証データが記憶されることとなる。この結果、記憶装置100とホストシステム200との間で一对一の接続関係が成立される。従って、記憶装置100側では、ステップS23の処理を行うことにより、CPU12が、ディスク1のユーザデータへのアクセスを、ホストシステム200に対して許可することとなる。一方、ホストシステム200側は、記憶装置100から第2次認証データが送信されることを受けて、記憶装置100のディスク1のユーザデータへのアクセスが行える状態になったことを認識する。

【0034】なお、記憶装置100側において第2次認証データを記憶するタイミングを、ホストシステム200へ第2次認証データの送信を終了した後としているのは、ホストシステム200が第2次認証データを受取る前に誤ってホストシステム200の電源が切断され記憶装置100の方だけに第2次認証データが記憶されることを避けるためである。本発明では、記憶装置100のみに第2次認証データが記憶されている場合は、記憶装置100が、他のホストシステムにアクセスを許可している状態であることから、この他のホストシステム以外のホストシステムに対してはアクセスを不許可とするようにしている(この時の動作については後に詳述する)。このため、ホストシステム200の電源切断により記憶装置100側のみに第2次認証データが記憶されてしまうと、再度、記憶装置100とホストシステム200との間で認証処理を行う際に記憶装置100へのアクセスが不許可となってしまうという不具合が生じるが、上記したように記憶装置100での第2次認証データの記憶をホストシステム200への第2次認証データ送信時とすることで、そのような不具合を回避することができる。

【0035】また、上記したように設定した第2次認証データについて、記憶装置100及びホストシステム200から解除する方法は、従来のATAインターフェース仕様に記述されているセキュリティコマンドのパスワード解除の方法と同様である。即ち、ユーザにおいてホストシステム200から第2次認証データの消去を指示可能なコマンドを設けておき、ユーザからのコマンド指示に応じて、記憶装置100とホストシステム200との双方で、第2次認証データの記憶を消去するようにする。第2次認証データを消去する処理は、記憶装置100とホストシステム200との双方とも同じであり、第2次認証データを記憶している記憶領域全体に対して(00h)を書き込むことにより記憶内容を消去する。

(第2次認証データの比較動作) 上述したように第2次認証データを作成した後は、ホストシステム200側から記憶装置100に対して当該記憶装置100の電源が投入される際に、毎回、記憶装置100側で、双方に記憶されている第2次認証データを比較し、ホストシステム200に対してアクセスを許可するか否かを判断する

こととなる。この記憶装置 100 の第 2 次認証データの比較動作について、図 10 に示すフローチャートを参照して説明する。

【0036】記憶装置 100 に対して、ホストシステム 200 から、送信すべき第 2 次認証データのデータサイズ (512 バイト) を示す情報 (01h)、及び、第 2 次認証データ送信コマンド (F4h) が送信されると、図 11 のように、記憶装置 100 の HDC9 のセクタカウントレジスタには (01h)、コマンドレジスタには第 2 次認証データ送信コマンド (F4h) が書き込まれる。

【0037】CPU12 は、HDC9 のコマンドレジスタから第 2 次認証データ送信コマンド (F4h) を読出し (ステップ S31)、コマンド内容を確認する (ステップ S32)。コマンドが第 2 次認証データ送信コマンド (F4h) でない場合は、読み出された別のコマンドに対する処理を行なうが (ステップ S32 の No)、この場合は第 2 次認証データ送信コマンド (F4h) であると確認される (ステップ S32 の Yes)。

【0038】CPU12 は、ホストシステム 100 から送信される第 2 次認証データを受信してバッファメモリ 10 に記憶する。 (ステップ S33)。このとき、CPU12 は、エラー無く第 2 次認証データを受信したことをホストシステム 100 に報知すべく、HDC9 のエラーレジスタに (00h) を書き込む。

【0039】続いて、CPU12 は、ホストシステム 100 から送信された第 2 次認証データと記憶装置 100 側で記憶している第 2 次認証データ (即ち、ROM13 に記憶している第 2 次認証データ) とを比較する。ホストシステム 200 側の第 2 次認証データと記憶装置 100 側の第 2 次認証データとの比較の結果、一致していると判断した場合、CPU12 は、HDC9 のエラーレジスタに (00h) を書き込み、ホストシステム 200 に対してディスク 1 のユーザデータへのアクセスを許可する旨報知する。一方、一致していない場合は、HDC9 のエラーレジスタに (04h) を書き込み、ホストシステム 200 に対してディスク 1 のユーザデータへのアクセスを不許可とする旨を報知する (ステップ S34)。CPU12 は、HDC9 のエラーレジスタに第 2 次認証データの比較結果を書き込むと、ホストシステム 200 から送信された第 2 次認証データ送信コマンド (F4h) に対する第 2 次認証データの比較処理を終了する。

【0040】この後、ホストシステム 200 側では、HDC9 のエラーレジスタの内容が確認されるが、エラーレジスタの内容が (00h) の場合は、記憶装置 100 が双方の第 2 次認証データが一致したと判断し、ディスク 1 のユーザデータへのアクセスを許可したことを認識し、以降のディスク 1 のユーザデータへのアクセスを行える状態が取られる。一方、エラーレジスタの内容が (04h) の場合は、ホストシステム 200 側は、記憶

装置 100 が双方の第 2 次認証データが不一致としたと判断し、ディスク 1 のユーザデータへのアクセスを不許可としたことを認識し、以降の記憶装置 100 のディスク 1 のユーザデータへのアクセスを行わない状態を取る。そして、ホストシステム 200 側は、図示せぬ表示画面等において記憶装置 100 へのアクセスが不許可となった旨をユーザに通知する。

(ホストシステム側の認証処理) 次に、ホストシステム 200 側の認証処理について、以下に説明する。

【0041】ホストシステム 200 は、パーソナルコンピュータや汎用コンピュータ等の各種のコンピュータである。ホストシステム 200 は、図 12 に示すように、ATA インターフェース回路 21、CPU22、ROM23、RAM24、RTC25 等によって構成される。ATA インターフェース回路 21 は、ATA 規格のインターフェースにて、記憶装置 100 との間でのデータ転送を制御するものである。CPU22 は、ホストシステム 200 のメインの制御装置であり、ROM23 や、RAM24 に格納された制御プログラムに従って、認証処理を行う。また、ROM23 は、ホストシステム 200 の固有情報を記憶する。RAM24 は、第 2 次認証データを記憶する。RTC25 は、現在の日時情報を出力する。

【0042】ホストシステム 100 の認証処理を、図 13、14 を参照して説明する。

【0043】先ず、CPU22 は、記憶装置 100 に第 2 次認証データが記憶されているか否かを問い合わせるため、ATA インターフェース回路 21 を介して、記憶装置 100 に認証データ確認コマンド (8Dh) を送信する (ステップ S41)。次いで、CPU22 は、この認証データ確認コマンド (8Dh) に応答して記憶装置 100 の HDC9 のエラーレジスタに書き込まれた記憶内容を参照することで、記憶装置 100 に第 2 次認証データが記憶されているか否かを判断する (ステップ S42)。

【0044】記憶装置 100 の HDC9 のエラーレジスタの記憶内容が (00h) である場合、CPU22 は、記憶装置 200 では第 2 次認証データが記憶されていないと判断し (ステップ S42 の No)、次いで、ホストシステム 100 自身に第 2 次認証データを記憶しているか否かを判断するため、RAM24 に第 2 次認証データが記憶されているか否かを判断す (ステップ S43)。

【0045】ホストシステム 200 側にも第 2 次認証データが記憶されていない場合は (ステップ S43 の No)、ホストシステム 200 と記憶装置 100 とが共に第 2 次認証データを記憶していないこととなるため、この場合、ホストシステム 200 と記憶装置 100 との間に新たな接続関係を成立させて記憶装置 100 に対してアクセス許可を得るべく、以下に説明するステップ S44～ステップ S48 の処理を行う。

【0046】CPU22は、ROM23に記憶された固有情報とRTC25から出力される日時情報とに基づいて第1次認証データ(図6)を作成する(ステップS44)。そして、CPU22は、作成した第1次認証データを記憶装置100に送信すべく、先ず、記憶装置100に、送信すべき第1次認証データのデータサイズ(512バイト)を示す情報(01h)を送信し、続いて、第1次認証データ送信コマンド(8Fh)を送信する。第1次認証データ送信コマンド(8Fh)を送信した後、CPU22は、第1次認証データを記憶装置100に送信する(ステップS45)。

【0047】次に、CPU22は、記憶装置100に対して当該記憶装置100で作成された第2次認証データを送信するように要求すべく、記憶装置100に第2次認証データのデータサイズ(512バイト)を示す情報(01h)を送信し、続いて、第2次認証データ受信コマンド(81h)を送信する(ステップS46)。記憶装置100が、第2次認証データ受信コマンド(81h)の送信に応答して第2次認証データを送信することを報知すべくHDC9のエラーレジスタを(00h)としたことを確認後、記憶装置100から送信される第2次認証データを受信し、RAM24に記憶する(ステップS47)。そして、CPU22は、記憶装置100が、当該記憶装置100のディスク1のユーザデータへのアクセスを許可したものと認識し、以降の記憶装置100へのアクセスを行える状態とする(ステップS48)。

【0048】一方、CPU22は、ステップS43の判断において、RAM24に第2次認証データが記憶されていると判断した場合は(ステップS43のYes)、ホストシステム200側のみ第2次認証データが記憶されていることとなるため、記憶装置100へのアクセスが不許可であると判断し、記憶装置100へのアクセスを行わない状態とする(ステップS49)。即ち、この場合、ホストシステム200が他の記憶装置に対するアクセスが行なえる状態となっているため、CPU22は、アクセスが許可されている他の記憶装置以外の記憶装置にはアクセスを行なえないよう制御すべく、今回アクセスしようとしている記憶装置100へのアクセスを不許可とする。

【0049】次に、上記したステップS42の判断で、記憶装置100に第2次認証データが記憶されていると判断した場合を以下に説明する。

【0050】CPU22は、ステップS42において、記憶装置100に第2次認証データが記憶されていると判断すると(ステップS42のYes)、次いで、ホストシステム200自身に第2次認証データが記憶されているか否かを判断する(ステップS50)。このステップS50の処理は、上述したステップS43と同様であり、CPU22がRAM24に第2次認証データが記憶

されているか否かを判断することで行う。このステップS50の判断で、ホストシステム200自身にも第2次認証データが記憶されていると判断した場合(ステップS50のYes)、ホストシステム200と記憶装置100共に、第2次認証データを記憶していることとなる。従って、この場合、CPU22は、ホストシステム200の記憶している第2次認証データが記憶装置100に記憶している第2次認証データと一致するか否かを確認すべく、送信すべき第2次認証データのデータサイズ(512バイト)を示す情報(01h)を送信し、続いて、第2次認証データ送信コマンド(F4h)を記憶装置100へ送信する。続いて、CPU22は、RAM24に記憶されている第2次認証データを記憶装置100へ送信する(ステップS51)。

【0051】次に、CPU22は、送信した第2次認証データに対する記憶装置100の比較結果を確認すべく当該記憶装置100のHDC9のエラーレジスタの記憶内容を参照する(ステップS52)。この結果、記憶装置100のHDC9のエラーレジスタの内容が(00h)の場合、CPU22は、記憶装置100がアクセスを許可したと認識し、以降の記憶装置100へのアクセスを行える状態とする(ステップS53)。一方、エラーレジスタの内容が(04h)の場合は、CPU22は、記憶装置100がアクセスを不許可としたことを認識する。そして、CPU22は、以降の記憶装置100のディスク1のユーザデータへのアクセスを行わない状態とし、図示せぬ表示画面等において記憶装置100へのアクセスが不許可となった旨をユーザに通知する(ステップS54)。

【0052】また、上述したステップS50において、ホストシステム200自身に第2次認証データを記憶していない場合(ステップS50のNo)は、記憶装置100が第2次認証データを記憶しているのに対して、ホストシステム200の方が第2次認証データを記憶していないこととなる。この場合、記憶装置200は、他のホストシステムに対してアクセス許可を与えている状態であるため、アクセス許可が与えられている他のホストシステム以外は、記憶装置100へのアクセスを不許可とする。従って、CPU22は、ステップS54の処理へ移り、記憶装置100へのアクセスは不許可とし、アクセス不許可の場合の処理を行う。

【0053】また、このようにホストシステム200側で認証処理を行った結果、記憶装置100へのアクセスが許可とされた場合は(ステップS48、若しくは、ステップS53)、ホストシステム200のCPU22は、以降の処理において記憶装置100へアクセスし、ユーザデータの読み書きを行うこととなる。

【0054】以上説明したように、記憶装置100とホストシステム200との間で、互いの固有情報を用いて、共同して第2次認証データを作成し、このデータを

用いて互いの認証を行うようにしたため、記憶装置側においては、当該記憶装置へのアクセスを特定のホストシステムのみに限定するよう制御でき、また、ホストシステム側においては、特定の記憶装置のみに限定してアクセスを行うよう制御することが可能となる。

【0055】なお、上述した本実施形態では、記憶装置100やホストシステム200の固有情報として、メーカー名、機種名、シリアル番号を用いているが、これに限らず、同一機種（若しくは類似機種を含めて）で全て異なるような数値（若しくは統計的に同一となる確立が非常に低い数値）を採用しても良い。更には、ユーザによって解析できないように固有情報を暗号化しても良い。

（第2の実施の形態）上述した実施形態では、ホストシステム200側で第1次認証データを作成し記憶装置100側で第2次認証データを作成するようにしているが、これとは逆に、記憶装置100側で第1次認証データを作成しホストシステム200側で第2次認証データを作成するようにしても良い。この第2の実施の形態について、以下に説明する。

【0056】ここでは、まず、ホストシステム200側が、ホストシステム200側及び記憶装置100側に第2次認証データが記憶されているか否かを判断するが、この判断においてホストシステム200側が、ホストシステム200側にも記憶装置100側にも第2次認証データが記憶されていないと判断した場合に、以下のような第2次認証データの作成動作を行なう。

【0057】即ち、ホストシステム200のCPU22が、第1次認証データを作成するよう指示すべく記憶装置100に対して第1次認証データ作成指示コマンドを送信する。記憶装置100側のCPU12では、その第1次認証データ作成指示コマンドを受けて、ROM13に記憶されている記憶装置100の固有情報に基づいて第1次認証データを作成し、一次的にCPU12内の図示しないRAMに記憶する。

【0058】次いで、ホストシステム200側のCPU22が、第1次認証データの送信を要求すべく記憶装置100に対して第1次認証データ受信コマンドを送信する。記憶装置100側のCPU12では、その第1次認証データ受信コマンドを受けて、図示しないCPU12内のRAMに記憶している第1次認証データをホストシステム200側へ送信する。

【0059】ホストシステム200側のCPU22は、記憶装置100側から第1次認証データを受信すると、この第1次認証データとROM23に記憶された固有情報とRTC25から出力される日時情報とに基づいて第2次認証データを作成し、RAM24に記憶する。次いで、ホストシステム200側のCPU22は、作成した第2次認証データを送信すべく記憶装置100に対して第2次認証データ送信コマンドを送信し、次いで、第2次認証データを送信する。

【0060】記憶装置100側のCPU12では、第2次認証データ送信コマンドを受けると、この第2次認証データ送信コマンドに続いてホストシステム200側から送信される第2次認証データを受信し、ROM13に記憶する。そして、第2次認証データをROM13に記憶した後、記憶装置100側のCPU12は、HDC9のエラーレジスタに(04h)をセットすることで、ホストシステム200にエラー無く第2次認証データを受信したことを報知する。

【0061】ホストシステム200側のCPU22では、記憶装置100側からエラー無く第2次認証データを受信した旨の報知を受けると、記憶装置100側が、当該記憶装置100のディスク1のユーザデータへのアクセスを許可したものと認識し、以降の記憶装置100へのアクセスを行える状態とする。

【0062】なお、第2次認証データの作成動作以外の処理動作、即ち、第2次認証データを作成するよりも前に、ホストシステム200が当該ホストシステム200及び記憶装置100に第2次認証データが記憶されているか否かを判断する場合の処理動作や、第2次認証データを作成した後の記憶装置100とホストシステム200との間の第2次認証データの認証を行なう場合の処理動作等は、上述した第1の実施の形態の場合と同様である。

【0063】

【発明の効果】以上詳述したように本発明によれば、記憶装置或いはホストシステム的一方で作成された認証データに基づいて他方がアクセス制御用の認証データを作成し、この認証データを用いてホストシステムのアクセス制御を行なうようにしたため、記憶装置側において、当該記憶装置へのアクセスを特定のホストシステムのみに限定するよう制御できる。

【図面の簡単な説明】

【図1】本発明の実施形態に係る記憶装置の構成を示した図。

【図2】認証データ確認コマンド(8Dh)が書き込まれた時のHDC9の各種レジスタの内容を示す図。

【図3】記憶装置の第2次認証データの記憶有無の確認動作を示すフローチャート。

【図4】記憶装置の第2次認証データの作成動作を示すフローチャート。

【図5】第1次認証データ送信コマンド(8Fh)が書き込まれた時のHDC9の各種レジスタの内容を示す図。

【図6】ホストシステムで作成される第1次認証データを示す図。

【図7】記憶装置で作成される第2次認証データを示す図。

【図8】記憶装置の第2次認証データの送信動作を示すフローチャート。

【図9】第2次認証データ受信コマンド(81h)が書き込まれた時のHDC9の各種レジスタの内容を示す図。

【図10】記憶装置の第2次認証データの比較動作を示すフローチャート。

【図11】第2次認証データ送信コマンド(F4h)が書き込まれた時のHDC9の各種レジスタの内容を示す図。

【図12】本発明の実施形態に係るホストシステムの構成を示す図。

【図13】本発明の実施形態に係るホストシステムの認証処理を示すフローチャート。

【図14】本発明の実施形態に係るホストシステムの認証処理を示すフローチャート。

【符号の説明】

1…ディスク

2…SPM

3…ヘッド

4…アクチュエータ

5…VCM

6…SPM/VCMドライバ

7…ヘッドアンプ回路

8…リード/ライトチャネル

9…HDC

10…バッファメモリ

11…ゲートアレイ回路

12…CPU(記憶装置側)

13…ROM(記憶装置側)

21…ATAインターフェース回路

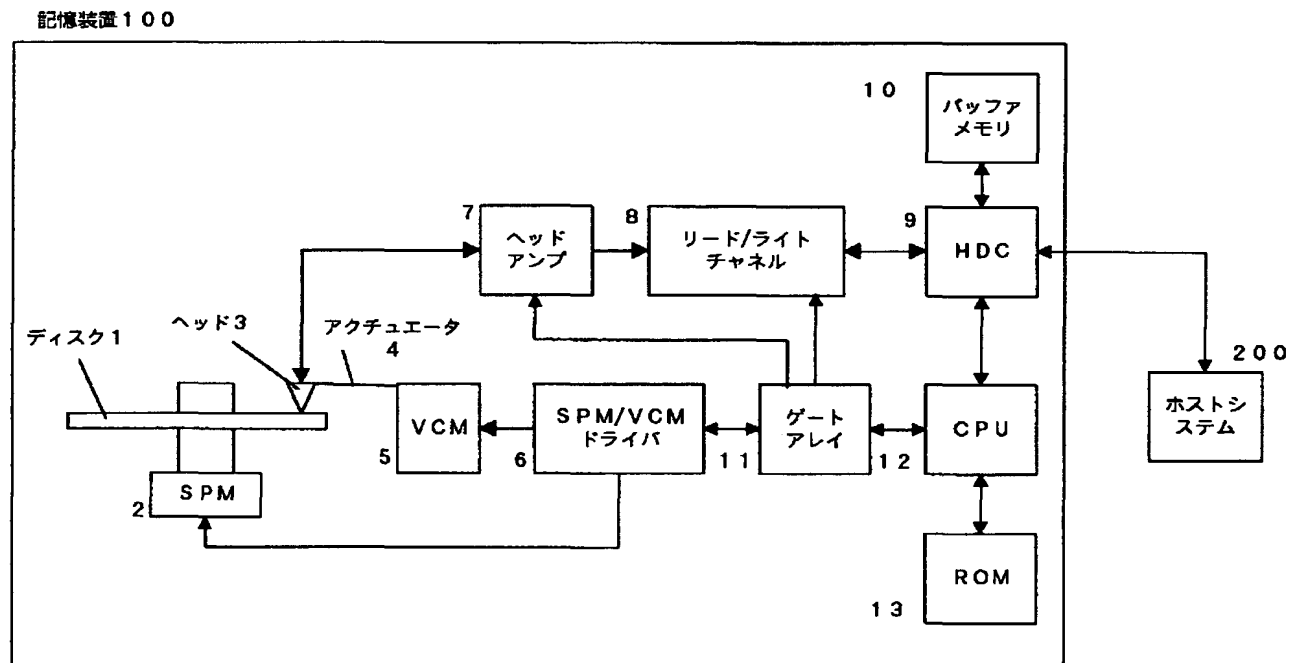
22…CPU(ホストシステム側)

23…ROM(ホストシステム側)

100…記憶装置

200…ホストシステム

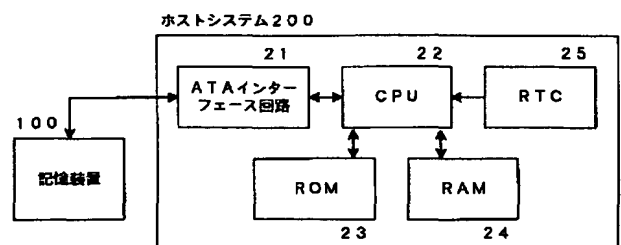
【図1】



【図6】

【図12】

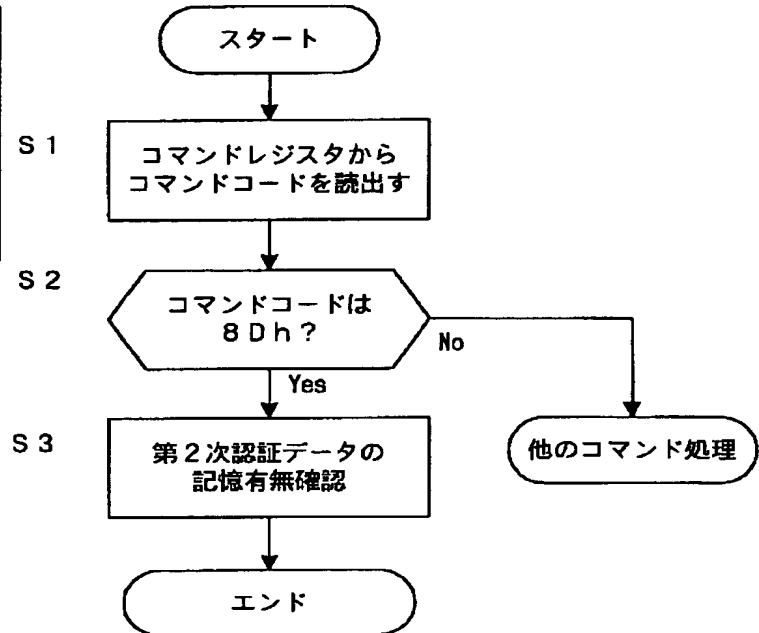
0000h 54h 4Fh 53h 48h 49h 42h 41h 2Ch 53h 61h 74h 65h 6Ch 6Ch 69h 74h
 "T" "O" "H" "S" "I" "B" "A" "S" "a" "t" "e" "I" "T" "i" "t"
 0010h 65h 32h 35h 35h 30h 68h 2Ch 31h 89h 89h 39h 2Dh 30h 39h 2Dh 31h
 "e" "2" "5" "5" "0" "X" "I" "9" "9" "9" "-" "0" "9" "-" "1"
 0020h 33h 2Ch 31h 39h 3Ah 34h 30h 3Ah 30h 30h 00h 00h 00h 00h 00h
 "3" "2" "1" "9" "4" "0" "0" "0" "0"
 0030h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h
 (0030h~01FFhまでのデータは全て「00h」)
 01FFh 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h



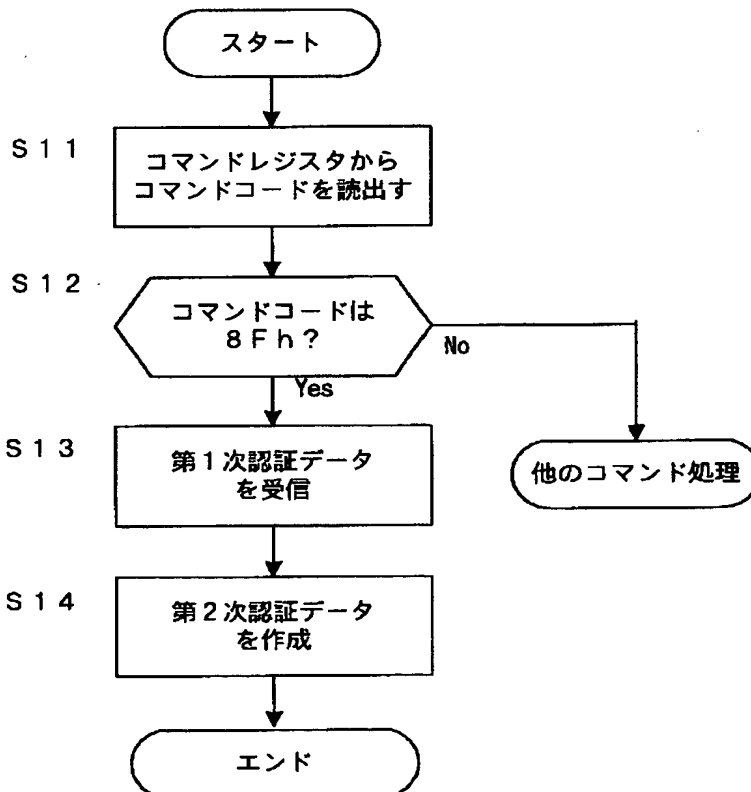
【図2】

レジスタ名	設定値
コマンドレジスタ	8Dh
セクタナンバレジスタ	(規定しない)
シリンダ・ロウレジスタ	(規定しない)
シリンダ・ハイレジスタ	(規定しない)
セクタカウントレジスタ	(規定しない)
ドライブ・ヘッドレジスタ	(規定しない)
フィーチャーレジスタ	(規定しない)
エラーレジスタ	04h

【図3】



【図4】



【図5】

レジスタ名	設定値
コマンドレジスタ	8Fh
セクタナンバレジスタ	(規定しない)
シリンダ・ロウレジスタ	(規定しない)
シリンダ・ハイレジスタ	(規定しない)
セクタカウントレジスタ	01h
ドライブ・ヘッドレジスタ	(規定しない)
フィーチャーレジスタ	(規定しない)
エラーレジスタ	00h

【図9】

レジスタ名	設定値
コマンドレジスタ	81h
セクタナンバレジスタ	(規定しない)
シリンダ・ロウレジスタ	(規定しない)
シリンダ・ハイレジスタ	(規定しない)
セクタカウントレジスタ	01h
ドライブ・ヘッドレジスタ	(規定しない)
フィーチャーレジスタ	(規定しない)
エラーレジスタ	00h

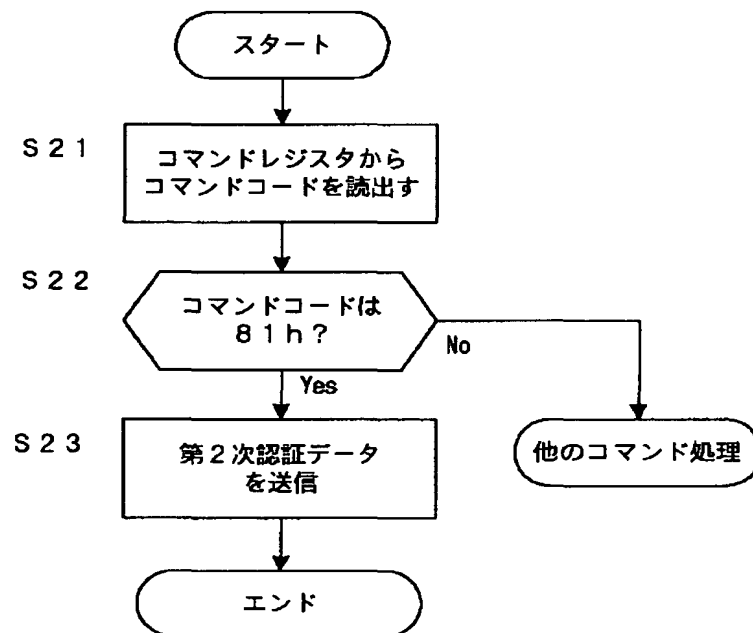
【図7】

0000h 54h 4Fh 53h 48h 49h 42h 41h 2Ch 53h 61h 74h 65h 6Ch 6Ch 69h 74h
 "T" "O" "H" "S" "I" "B" "A" " " "S" "a" "c" "e" "I" "I" "I" "c"
 0010h 65h 32h 35h 35h 30h 58h 2Ch 31h 39h 39h 39h 2Dh 30h 39h 2Dh 31h
 "e" "2" "5" "5" "0" "X" " " "I" "9" "9" "9" " " "0" "9" " " "1"
 0020h 33h 2Ch 31h 39h 3Ah 34h 30h 3Ah 30h 30h 00h 00h 00h 00h 00h 00h
 "3" " " "I" "9" " " "4" "0" "0"
 0030h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h
 (0030h~00FFhまでのデータは全て「00h」)
 00FFh 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h
 0100h 54h 4Fh 53h 48h 49h 42h 41h 2Ch 4Dh 4Bh 36h 34h 31h 31h 4Dh 4Ah
 "T" "O" "H" "S" "I" "B" "A" " " "M" "K" "6" "4" "I" "I" "M" "A"
 0110h 54h 2Ch 5Ah 38h 47h 35h 30h 38h 39h 31h 47h 00h 00h 00h 00h 00h
 "T" " " "Z" "8" "G" "5" "0" "8" "9" "I" "G"
 0120h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h
 (0120h~01FFhまでのデータは全て「00h」)
 01FFh 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h 00h

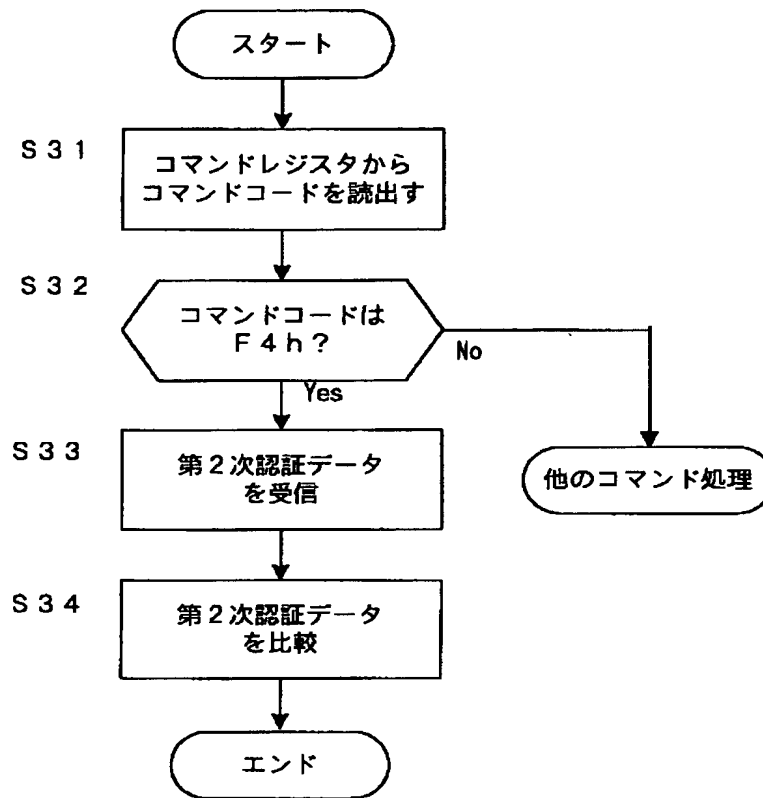
【図11】

レジスタ名	設定値
コマンドレジスタ	F 4 h
セクタナンバレジスタ	(規定しない)
シリンダ・ロウレジスタ	(規定しない)
シリンダ・ハイレジスタ	(規定しない)
セクタカウントレジスタ	0 1 h
ドライブ・ヘッドレジスタ	(規定しない)
フィーチャレジスタ	(規定しない)
エラーレジスタ	0 0 h

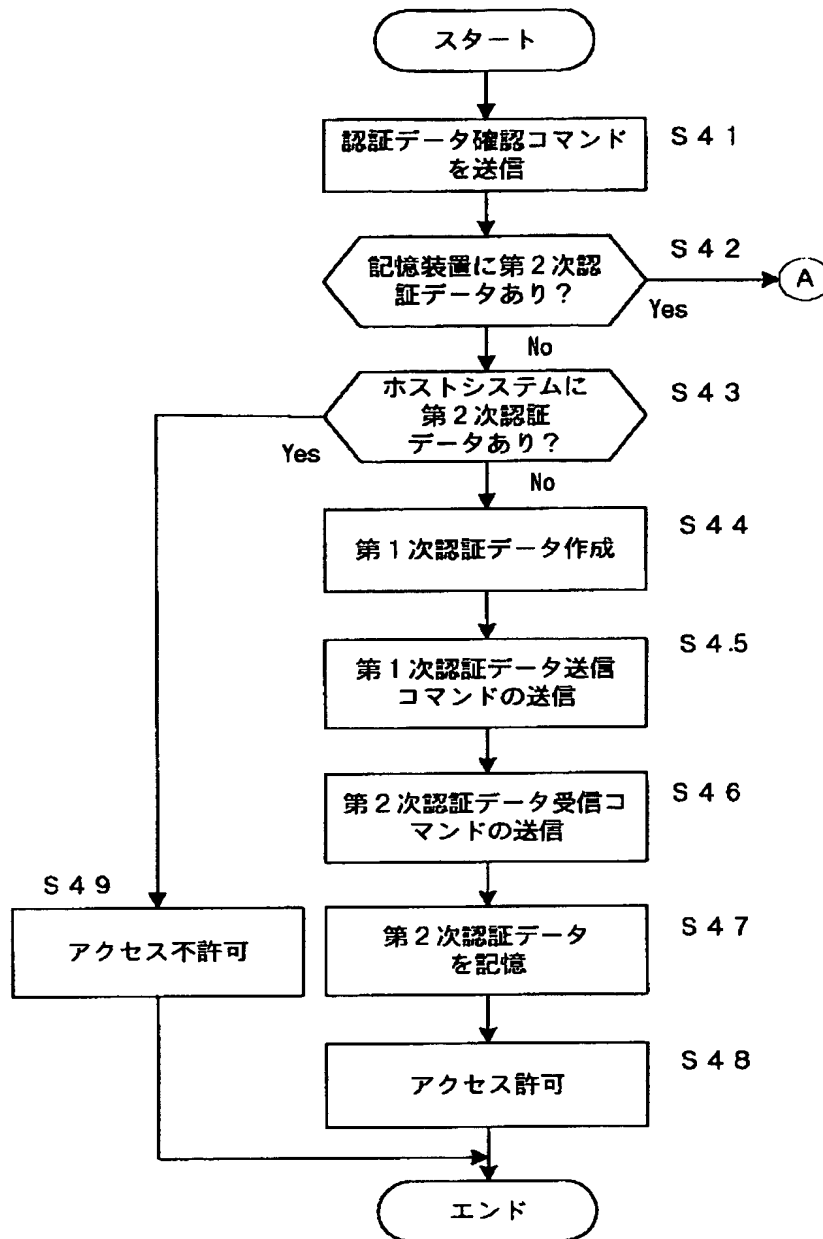
【図8】



【図10】



【図13】



【図14】

